Partilha Ficheiros – SSH/SCP/SFTP

1. SSH

O protocolo SSH permite a transferência de dados de forma segura (SSL). Utilizando a criptografia de chave pública que o SSH usa é possível determinar se um computador remoto ou um utilizador é autêntico. Por defeito o SSH *server* fica à escuta no porto 22.

O SSH permite gerar o par chave pública e chave privada. Cedendo a chave pública é possível aceder a um sistema remotamente sem necessidade de digitar a *password*. Exemplificando o processo:

Gerar chaves do utilizador **aluno1** no host**A**

```
ssh-keygen -t rsa
```

- Serão criados 2 ficheiros em `~aluno1/.ssh/`
  - `id_rsa` → contém a chave privada do utilizador aluno1
  - `id_rsa.pub` → contém a chave pública do utilizador aluno1

Supondo que no **hostB** existe um utilizador **facturas**, vamos fornecer a chave pública do **aluno1@hostA**

- `cd ~facturas/.ssh/`
- `vi authorized_keys`
  - paste da chave pública do aluno1 que foi transferida/copiada do **hostA** para o **hostB**
- Dar permissões ao ficheiro `authorized_keys`**:** user=**r+w**, grupo=**r**, outros=**r**
- As permissões do diretório .ssh devem estar a 700

Experimentar agora aceder ao do **hostA** (user: **aluno1**) ao **hostB** à conta **facturas**:

- No hostA: `ssh facturas@hostB`

Para além do comando `ssh` existe o `scp` e `sftp`. Todos comunicam através da porta 22 de forma cifrada.

Obs: Explore o comando ssh-copy-id para a transferência de chaves